THE GROUPS OF ORDER p^m WHICH CONTAIN EXACTLY p CYCLIC SUBGROUPS OF ORDER p^α*

BY

G. A. MILLER

If a group (G) of order p^m contains only one subgroup of order p^α, $\alpha > 0$, it is known to be cyclic unless both $p = 2$ and $\alpha = 1$.† In this special case there are two possible groups whenever $m > 2$. The number of cyclic subgroups of order p^α in G is divisible by p whenever G is non-cyclic and $p > 2$.‡ In the present paper we shall consider the possible types of G when it is assumed that there are just p cyclic subgroups of order p^α in G. That is, we shall consider the totality of groups of order p^m which satisfy the condition that each group contains exactly p cyclic subgroups of order p^α. It is evident that $\alpha < m$.

Since the total number of subgroups of order p^α in G is of the form $1 + kp$, it follows that $\alpha > 1$. For all values of α greater than unity there is at least one group of order p^m which contains exactly p cyclic subgroups of order p^α, viz., the abelian group of type $(m - 1, 1)$. When p is odd there is a non-abelian group which is conformal with this abelian group. It will be proved that these two groups are the only groups of order p^m, $p > 3$, which contain exactly p cyclic subgroups of order p^α. These two groups exist also when $p = 3$ or 2 and $m > 3$, but they are not the only groups which contain p cyclic subgpoups of order p^α, $p = 2$. When $\alpha = 2$ and $m = 4$ there is another group of order 3^m which contains just 3 cyclic subgroups of order 9.

Let the p cyclic subgroups of order p^α be represented by $P_1, P_2, \cdots, P_p$. Each of these transforms every other one into itself. The group generated by any two of them contains all the others, since it cannot be cyclic. Let s_1, s_2, be generators of P_1, P_2, respectively. From the fact that $s_1^{-1} s_2 s_1 = s_2^\beta$ and $s_1^{-1} s_1 s_2 = s_1^\gamma$, it follows that the commutator subgroup of the group (K) generated by s_1, s_2, is composed of operators which are invariant under this group. The order of this commutator subgroup cannot exceed p since $s_1^p = s_2^{\gamma p}$. This

*Presented to the Society (Chicago) December 30, 1905. Received for publication December 28, 1905.

†BURNSIDE, *Theory of groups of finite order*, 1897, p. 75.

‡Proceedings of the London Mathematical Society, vol. 2 (1904), p. 142.

last equation results directly from the fact that G contains only p cyclic subgroup of p^α; for if it were not satisfied, s_1^p and s_2 would generate a group which would contain at least p cyclic subgroups of order p^α without containing s_1.

From the given equations it follows that the order of K is $p^{\alpha+1}$ and that K is one of the two groups of this order which contain p cyclic groups of order p^α. The only exception to this is when both $\alpha = 2$ and $p = 2$. In this special case K is completely determined by the given conditions, being the abelian group of order 8 and of type (2, 1). This establishes the following theorem: *If a group of order p^m contains exactly p cyclic subgroups of order p^α, these subgroups generate a characteristic subgroup of order $p^{\alpha+1}$, which is either the abelian group of type $(\alpha, 1)$, or the non-abelian group which is conformal with this abelian group.*

We shall now prove that K is abelian whenever G contains operators whose order exceeds p^α. If s is such an operator it may be assumed without loss of generality that $s^p = s_1$. Since there are only $p - 1$ other cyclic subgroups of order p^α it follows that $s^{-1}s_2 s = cs_2 = s_2^\gamma$. The order of c cannot exceed p as $s_2^p = s_1^{\gamma p} = s^{\gamma p^2}$. Hence $s^p = s_1$ is commutative with s_2 or K is abelian. This theorem applies to every value of p. It should be observed that K contains just $p + 1$ subgroups of every order. As each of the non-cyclic subgroups in K is characteristic, it follows that any operator (t) of order p^γ, which transforms K into itself, transforms any operator s of K such that if $t^{-1}st = c_1 s$, $t^{-1}c_1 t = c_2 c_1$, $t^{-1}c_2 t = c_3 c_2$, $\cdots$, then the order of c_1 is less than that of s, the order of c_2 is less than that of c_1, $\cdots$ When $c_{\alpha-1}$ is of order p^2 and c_α is of order p it is possible that $c_{\alpha+1}$ is also of order p. This special case will be considered in what follows.

Let t be any operator of order p^γ, $\gamma < \alpha$, which transforms K into itself and such that t^p is in K, and consider the order of the product ts_1, where s_1 has the same meaning as above. We have

$$(ts_1)^p = ts_1 ts_1 ts_1 \cdots p \text{ times} = ts_1 t^{-1} t^2 s_1 t^{-2} t^3 s_1 t^{-3} \cdots t^p$$

$$= c_1 s_1 c_2 c_1^2 s_1 c_3 c_2^3 c_1^3 s_1 \cdots = s_1^p k,$$

where k is the product of operators of lower order contained in K whenever $p > 3$. Hence the order of ts_1 is the same as that of s_1, viz., p^α whenever $p > 3$. This proves that G contains no operators whose orders divide p^α except those which are included in K, unless $p = 3$ or 2.

When $p = 3$ the above equations remain true whenever $\alpha > 2$. That is, if a group of order 3^m contains only 3 cyclic subgroups of order p^α, $\alpha > 2$, the group generated by these cyclic subgroups includes all the operators of the group whose orders divide p^α. We shall now consider the case when G contains operators whose orders exceed p^α. We shall again assume that $s^p = s_1$. The group (K_1) generated by s and K is known to be conformal with the abelian group of type $(\alpha+1, 1)$.

If G should contain an operator (t) of order $p^{\alpha+1}$ which is not included in K_1 it could be assumed that $t^{-1}Kt = K$, and that $t^{p^2} = s_1^{ap}$. Just as above it may be seen that $(st)^p = s^p t^p$ into operators of lower order contained in K. As K is abelian it follows that $(st)^{p^2} = s_1^p s_1^{ap}$ into operators of lower order. By taking $a = -1$ it results that st is of a lower order than s. As this is impossible, K_1 includes all the operators of G whose orders divide $p^{\alpha+1}$. Hence we have the important result: *If a group of order* p^m, $p > 3$, *contains exactly* p *cyclic subgroups of order* p^α *it is either the abelian group of type* $(m-1, 1)$, *or the non-abelian group which is conformal with this abelian group.* When $\alpha > 2$, this theorem has also been proved for groups of order 3^m.

We shall now consider the groups of order 3^m which contain exactly 3 cyclic subgroups of order 9. If such a group contains also operators of order 27 it is conformal with the abelian group of type $(m-1, 1)$. This statement may be proved as follows. Let s be such an operator of order 27 and suppose that $s^3 = s_1$. The group of order 81 generated by s, s_2 is clearly conformal with the abelian group of type $(3, 1)$. If G contained an operator (t) of order 3 which is not found in this subgroup but transformed this subgroup into itself we should have $t^{-1}st = cs$, where c is of a lower order than s. Hence also $t^{-1}s^p t = (cs)^p = c^p s^p$. As t is commutative with c^p it follows that ts^p is of order p^2, contrary to the hypothesis that G contains only 3 cyclic subgroups of order 9. This proves the theorem. If a group of order 3^m contains only 3 cyclic subgroups of order 9 but contains also operators of order 27, it contains exactly four subgroups of order 3.

Suppose that G should contain an operator (t_1) of order 27 which is not contained in the group generated by s, s_2 but transforms this group into itself. It may be assumed that $t_1^9 = s^{-9}$. We have

$$(ts)^3 = tststs = tst^{-1}t^2st^{-2}t^3st^{-3}t^3 = c_1sc_2c_1^2sc_3c_2^3c_1^3s \cdot t^3 = s^3t^3k,$$

where k is of lower order than s^3t^3 and is commutative with s^3 and t^3. Hence $(ts)^9 = 1$, as s^3 and t^3 are also commutative. From this and the preceding paragraph it follows that all the operators of order 27 which are found in G are included in the group generated by s, s_2. That is, if G contains only 3 cyclic subgroups of order 9 but contains also operators of order 27, it also contains just 3 cyclic subgroups of order 27, and hence just 3 cyclic subgroups of every order which divides p^{m-1} and exceeds p.

The two preceding paragraphs prove that if a group of order 3^m contains just 3 cyclic subgroups of order 9 it is either conformal with the abelian group of type $(m-1, 1)$ or it contains only operators of order 3 in addition to the 18 of order 9 which are found in the 3 cyclic subgroups of order 9. In the latter case its order is 81; for if its order exceeded 81 each cyclic subgroup of order 9 would be transformed into itself by at least 81 operators of G. There would therefore be operators of order 3 which would transform each cyclic subgroup of order 9 into itself but would not be in the group of order 27 generated by these cyclic subgroups. As such an operator would give rise to additional operators of order 9 this is impossible. Hence we have the result: If a group of order 3^m contains exactly 3 cyclic subgroups of order 3^α, $\alpha > 2$, it contains exactly 3 cyclic subgroups of each of the orders $9, 81, \cdots, 3^{m-1}$, and hence is conformal with the abelian group of type $(m-1, 1)$. When $\alpha = 2$ and $m > 4$ the same conclusions hold. When $\alpha = 2$ and $m = 4$ there is another group which contains exactly 18 operators of order 9, viz., the group which contains only operators of order 3 besides the identity and these operators of order 9.

Combining these results with those which precede we have that a group of order p^m, $p > 2$, which contains just p cyclic subgroups of order p^α contains just p cyclic subgroups of each of the orders $p^2, p^3, \cdots, p^{m-1}$. The only exception to this which may arise is when $p = 3$ and $m = 4$. In this special case there is a group which contains just p cyclic subgroups of order p^2 without also containing any cyclic subgroups of order p^3. In this case, there are therefore three groups of order p^m which contain just p cyclic subgroups of order p^α while in all other cases there are only two such groups. It remains to consider the cases when $p = 2$.

We shall first prove that if a group of order 2^m contains just two cyclic subgroups of order 2^α, $\alpha > 2$, it cannot contain more than two cyclic subgroups of any higher order. It has already been proved that these two cyclic subgroups generate a group K of order $2^{\alpha+1}$ and that K is abelian whenever G contains operators of order $2^{\alpha+1}$. Suppose that t_1 is an operator such that $t_1^2 = s_1$. The group generated by t_1, s_2 is of order $2^{\alpha+2}$ and is either abelian or contains a commutator subgroup of order 2, generated by s_1.

If t_2 is another operator of order $2^{\alpha+1}$ contained in G we may assume that it transforms the given subgroup of order $2^{\alpha+2}$ into itself since G contains at least one operator of order $2^{\alpha+1}$ which has this property as every subgroup is invariant under a larger subgroup. We may assume that $t_2^4 = s_1^{-2}$. Hence $(t_1 t_2)^2 = t_1 t_2 t_1 t_2^{-1} t_2^2 = c t_1^2 t_2^2$, where c, t_1^2, t_2^2 are commutative and c is of a lower order than t_1^2. The order of $t_1 t_2$ is therefore less than 2^α. As $t_1 t_2$ transforms an operator of order 2^α in K into itself multiplied by an operator whose order does not exceed 2, the group generated by K and $t_1 t_2$ would contain more than two cyclic subgroups of order 2^α. As this is impossible it has been proved that a group of order 2^m which contains only two cyclic subgroups of order 2^α, $\alpha > 2$, contains at most two cyclic subgroups of order $2^{\alpha+1}$. If it contains only two such subgroups they generate a group of order $2^{\alpha+2}$ which is either abelian or contains a commutator subgroup of order 2.

We proceed to prove the theorem: *If a group of order* 2^m *contains exactly two cyclic subgroups of order* 2^β *but no cyclic subgroup of any higher order, then* $m \leqq 2^{\beta+2}$. It has been proved that the two cyclic subgroups of order 2^β generate a group of order $2^{\beta+1}$ whose commutator subgroup is generated by $s_1^{2^{\beta-1}}$. Suppose that $m > 2^{\beta+2}$ and let t_1, t_2 be any operators of G which are not also in K, $t_1^{-1}s_1t_1 = c_1s_1$, $t_2^{-1}s_1t_2 = c_2s_1$. The orders of c_1, c_2 cannot be less than $2^{\beta-1}$, since G does not involve any operator of order 2^β besides those in K.* It has also been observed that these orders cannot exceed $2^{\beta-1}$ since t_1, t_2 transform K into itself. From $(t_1t_2)^{-1}s_1t_1t_2 = c_3s_1$, where c_3 is of a lower order than c_1, c_2, it follows that t_1t_2 is in K. That is, the value of m does not exceed $2^{\beta+2}$.

The preceding results prove that if a group of order 2^m contains exactly two cyclic subgroups of order 2^α, $\alpha > 2$, it contains operators of order 2^{m-2} and hence has been determined.† It remains to consider the case when a group contains only two cyclic subgroups of order 4 and to prove that in this case it must also contain operators of order 2^{m-2}. If s_1 is an operator of largest order in such a G, the cyclic group which it generates is transformed into itself by each of the operators of order 4. Hence the group K generated by s_1 and these operators of order four is of order $2^{\beta+1}$, 2^β being the order s_1, and K is conformal with the abelian group of type $(\beta, 1)$.

If the order of G should exceed $2^{\beta+2}$, K would be transformed into itself by an operator t of order 8 such that the order of c in $t^{-1}s_1t$ could not exceed $2^{\beta-2}$. The order of the product of t into some operator of order 8 in K could therefore not exceed 4. As this is impossible it has been proved that *every group of order* 2^m *which contains exactly two cyclic subgroups of a given order contains a cyclic subgroup of order* 2^{m-2}.

If we combine this result with those which precede we arrive at the theorem: Every group of order p^m, p being any prime, which contains exactly p cyclic subgroups of the same order must contain a cyclic subgroup of order p^{m-2}. When p is odd and $m > 4$, we have the stronger theorem: Every group of order p^m which contains exactly p cyclic subgroups of the same order contains exactly p cyclic subgroups of every order from p^2 to p^{m-1}. This theorem is also true when $m = 3$, and when $m = 4$ and $p > 3$. As all the groups of order p^m which contain a cyclic subgroup of order p^{m-2} are known, these results give a complete determination of all the groups of order p^m which contain exactly p cyclic subgroups of the same order.

---

*Cf. Bulletin of the American Mathematical Society, vol. 7 (1901), p. 351.

†Transactions of the American Mathematical Society, vol. 2 (1901), p. 259; Bulletin of the American Mathematical Society, vol. 9 (1905), p. 494.